

From Compliance Artifacts to Continuous Cyber Assurance

An IL6 Case Study in Automated Security and cATO Readiness

DAFITC 2026 • Track 2: The Future of Cyber - Automated, Agile, and Assured

Joel Shuler • Morgan Ainslie • Platinum Technologies

PT78 | Mission-Focused Digital Engineering & Integration Partner

PT78 delivers mission-trusted digital capabilities in complex, high-risk environments.



Cybersecurity

We secure mission systems across the full stack.

- RMF and ATO execution and automation
- Secure system design and platform trust
- Cyber operations in restricted, high-scrutiny environments



AI You Can Actually Use

We design, deploy, and govern AI that delivers real value: securely, responsibly, and at scale.

- Mission-aligned AI solutions
- Responsible AI and governance implementation
- AI integration into enterprise platforms
- AI operations, monitoring, and optimization



Platform as a Service

We design and operate platforms that let teams deliver faster, more reliably, and at scale.

- Mission platforms and shared services
- Scalable application environments
- Integrated data, identity, and governance layers



X-Factor

We invest deliberately in differentiated capabilities that create operational and decision advantage.

- C2 technologies
- AI You Can Actually Use
- Data as a Service
- Evidence Intelligence and Vanguard

From mentor-protégé partnership to Vanguard

Platinum Technologies is the protégé in a Department of the Air Force Mentor-Protégé Program partnership with IBM, with Morgan State University as the mentor-protégé agreement partner. The partnership earned the FY2025 Nunn-Perry Award for strengthening the defense industrial base.

The capability development and technology transfer from that partnership is what Vanguard was built on.

Agenda



RMF promise | **Reality gap** | **Evidence model** | **IL6 case study** | **Lessons + Q&A**

Learning objectives

Explain why compliance-centric RMF struggles at software speed • Describe automated evidence and human-attested AI • Evaluate IL6 implementation approaches • Apply lessons learned to cATO readiness

The Promise of Risk Management and Compliance

DoD moved beyond DIACAP to manage cybersecurity risk throughout the system life cycle.

DIACAP → RMF → cATO readiness

Certification mindset

Periodic authorization packages and point-in-time accreditation activities.

Risk management framework

Categorize, select, implement, assess, authorize, and monitor as a disciplined lifecycle.

Continuous readiness

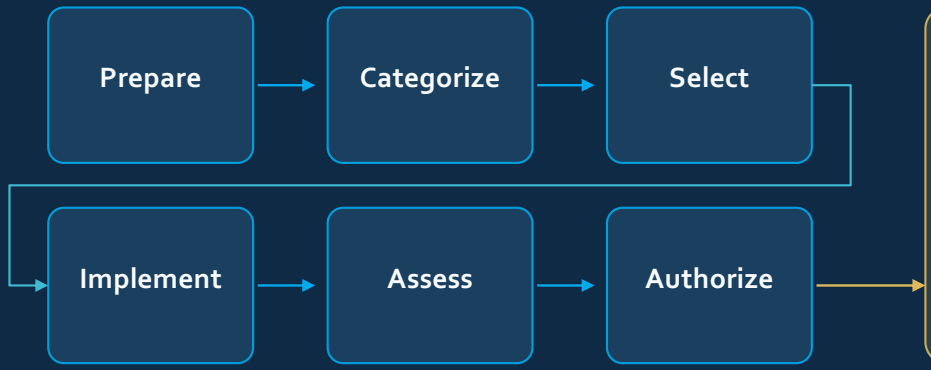
Authorization posture supported by ongoing evidence, active monitoring, and operational risk insight.



RMF is ultimately about mission assurance: trusted systems no matter the environment. Documentation serves that goal best when it produces continuously informed risk decisions.

RMF was designed to move at mission speed

NIST SP 800-37 Rev. 2: RMF promotes near real-time risk management and ongoing authorization through continuous monitoring.



Monitor

Monitor is where authorization stays tied to operational reality.

Ongoing risk visibility between formal assessments keeps security moving with delivery instead of gating it.

Then

Longer release cycles
Manual build/deploy steps
Assessment windows
Static infrastructure assumptions

Now

CI/CD pipelines
Software factories
Containers and dependencies
SBOMs and supply-chain gates
Frequent mission updates

Pressure point

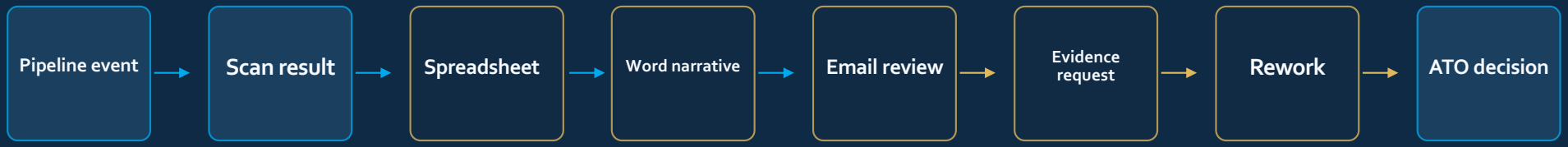
Security must be built into the delivery system.
Evidence must be presented as current and decision-ready.
Assurance has to keep pace to keep capability moving.

Security at the speed of mission

Run as designed, RMF should be an enabler of delivery tempo. The bottleneck is manual evidence work, not the framework itself.

What we actually experience

The real bottleneck is the manual path from security data to authorization-ready evidence, and authoritative public sources point to the same pattern.



Mission impact is not simply “late paperwork.” It is delayed capability, late risk visibility, analyst rework, and slower cyber response.

Hours spent reconciling evidence and chasing screenshots are hours not spent on risk, and delivery waits on the paperwork.

> DOD is still struggling to deliver new technologies quickly, even while faced with constantly evolving threats.
>
> GAO-24-106831, Weapon Systems Annual Assessment

> Legacy software acquisition and development practices do not provide the agility to deploy new software at the speed of operations.
>
> DoD Enterprise DevSecOps Reference Design

Security data already exists

The evidence is generated every day across the DevSecOps and cyber toolchain.

ACAS / Nessus
vulnerabilities

STIG / SCAP
configuration

SBOM
dependencies

Containers
image findings

CI/CD
pipeline gates

Inventory
assets

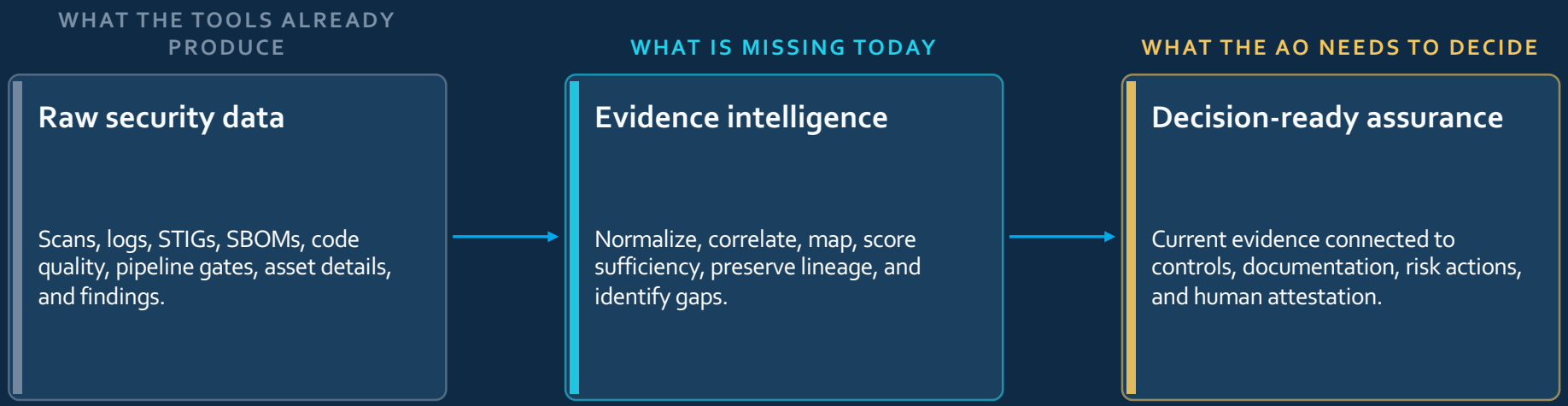
Logs
events

POA&M
risk actions

The data already exists; what is missing is maintained traceability from evidence to control claims, and that gap is what delays decisions.

Evidence Intelligence: The missing layer between data and evidence

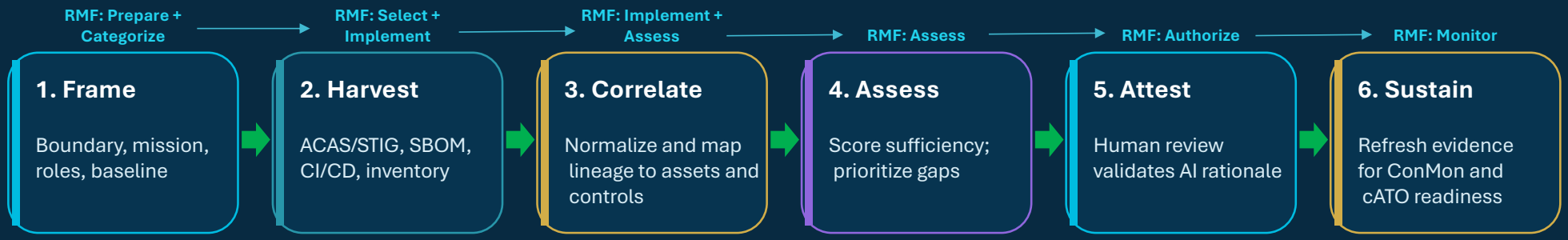
Scan results prove system state. They do not, by themselves, prove a control claim.



Vanguard was implemented to create this missing layer currently inside an IL6 boundary.

PT78 methodology: keeping every RMF step evidence-current

Each stage below carries an RMF step forward, so authorization rests on live security data instead of a point-in-time package.



Method principle

Automate the evidence collection and analysis chain so ISSOs, SCAs, PMs, and AOs can make faster, better-informed risk decisions for fielded Warfighter solutions.

VANGUARD operationalizes the method inside the IL6 boundary: ingest -> map -> analyze -> document -> monitor, with local AI as an advisory accelerator and human attestation as the governance control.

IL6 case study: Vanguard implementation

An automated cyber assurance platform deployed within the security boundary.

Operating constraint

Capability had to function within an IL6 / air-gapped context without exposing sensitive data to external services.

Design objective

Treat cybersecurity evidence as operational data, not disconnected documentation.

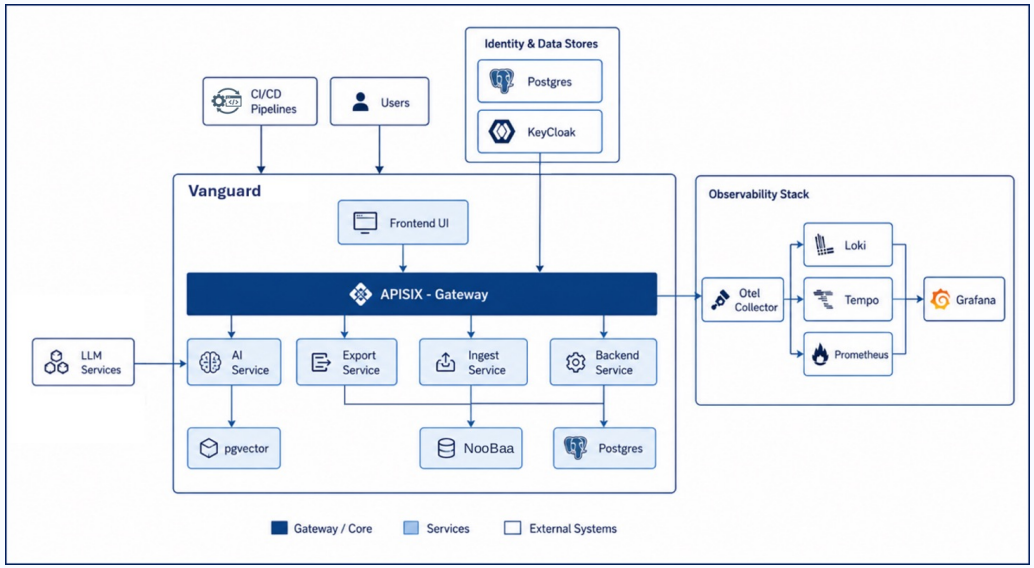
Governance principle

AI-generated findings are advisory and subject to human review, attestation, and RMF authority.

Vanguard views: Portfolio oversight • ISSO workbench • Assessment / SCA pre-adjudication

Vanguard reference architecture

Designed for IL6 / air-gap viability, accreditation readiness, and deployment flexibility.



Implementation choices

- React + TypeScript frontend
- Python/FastAPI microservices
- PostgreSQL + pgvector
- S3-style object storage
- APISIX gateway
- UBI / FIPS-enabled containers
- Keycloak OIDC/RBAC
- Local LLM model option

Automated evidence pipeline

Ingest, normalize, correlate, map, and present current evidence as an authorization model.



Evidence sources

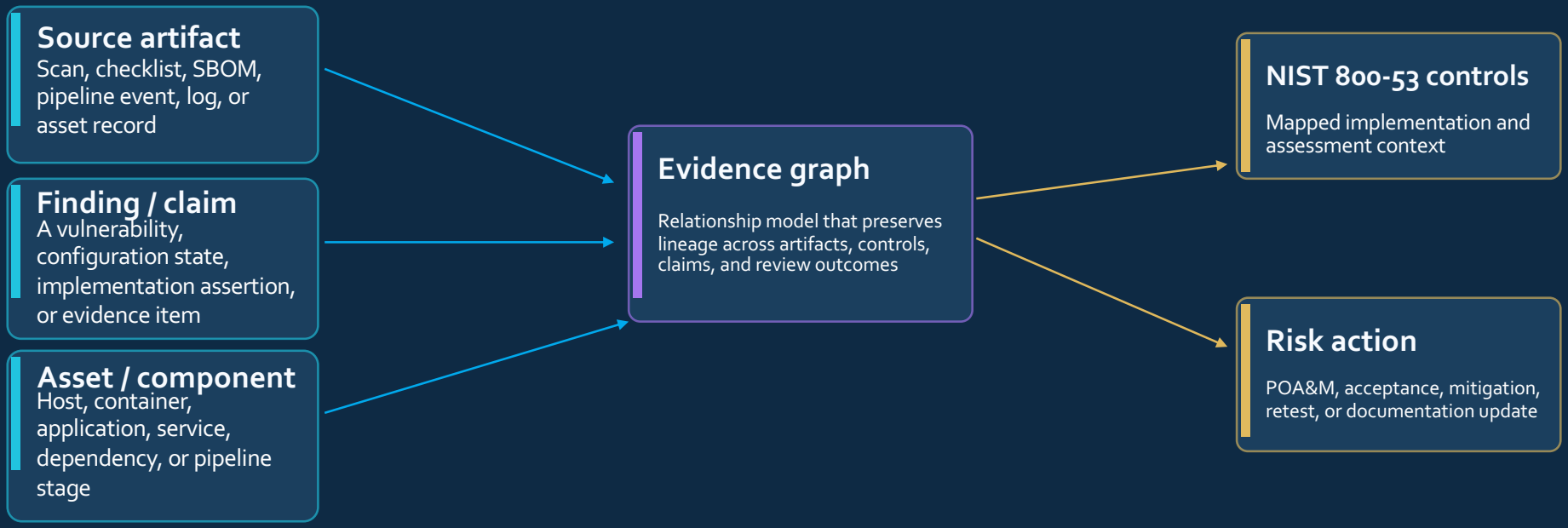
ACAS/Nessus, STIGs, SBOMs, container findings, asset inventories, CI/CD artifacts, pipeline gates, logs, and POA&M actions.

Evidence consumers

ISSO workbench, SCA pre-adjudication, AO posture views, SSP/SAR/SIA generation, and continuous monitoring dashboards.

Control correlation and evidence graph

The platform connects findings, artifacts, assets, and control claims so reviewers can follow the evidence trail.



Traceability makes automation defensible and reviews repeatable.

AI inside the security boundary

Local AI can accelerate analysis without moving sensitive evidence outside the enclave.

Local model option

On-prem / air-gapped deployment option with model-agnostic design and local LLM support.

Advisory analysis

Control gap identification, evidence sufficiency checks, SIA/SSP/SAR drafting, and impact analysis support.

Human attestation

Findings remain reviewable. Risk decisions and authorization authority remain with designated personnel.

AI assists the analyst so decisions come faster; authority stays with the AO.

Evidence sufficiency analysis

The question shifts from "Do we have an artifact?" to "Does this evidence support the control claim?"

Completeness

Do required artifacts exist and are they current?

Consistency

Do narratives, scans, assets, and diagrams tell the same story?

Traceability

Can a reviewer move from control claim to source evidence?

Sufficiency

Does the evidence prove the implementation assertion enough for review?

Vanguard evaluates documentation and artifact quality before the formal assessment cycle.

That enables early gap discovery and reduces rework when it is most expensive.

Documentation readiness

Documents become outputs of the evidence model not the only source of truth.

SSP

Narrative generation from current implementation evidence

SAR

Assessment narrative drafting and evidence linkage

SIA

Impact analysis support for system or environment changes

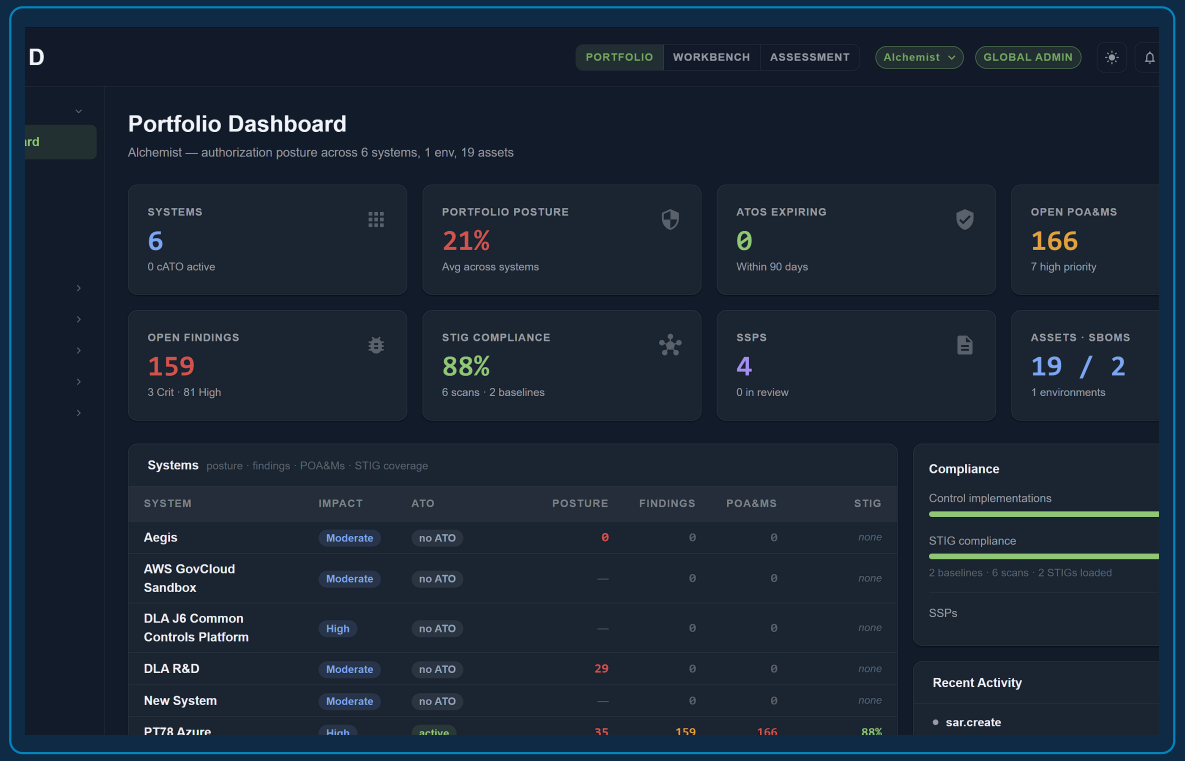
POA&M

Risk action tracking, aging, status, and retest context

The payoff is not a prettier document; it is a package that stays defensible between assessments.

Portfolio view: risk posture for leaders (DEMO)

A cross-system view changes the conversation from artifact status to mission-informed risk posture.

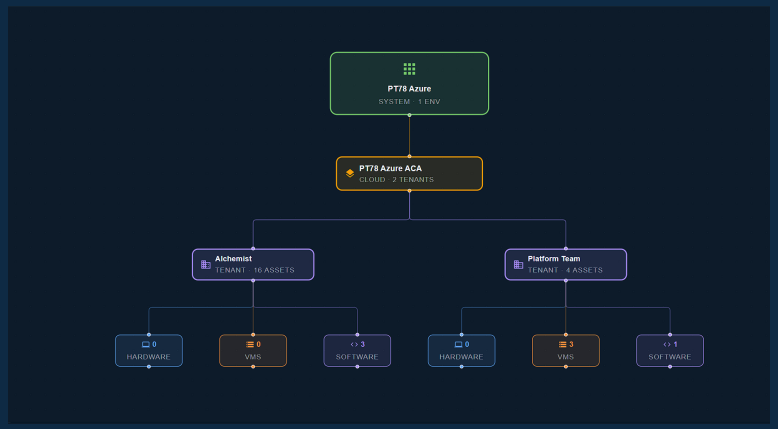


Leadership questions answered

Which systems are ready for review?
Where is risk accumulating?
Which findings are aging?
Where is evidence coverage weak?
What changed since the last decision?

Assessment view: traceability for reviewers

SCA and ISSO workflows need explainable AI and direct source evidence, not black-box conclusions.



Reviewer workflow

1. Select control or finding
2. Review evidence lineage
3. Inspect source artifact
4. Validate AI rationale
5. Attest, reject, or request remediation

Why it matters

Traceability reduces ambiguity, supports pre-adjudication, and helps teams find documentation gaps before formal review.

Continuous authorization readiness

The case study supports readiness for cATO but does not shortcut governance or authority.

TARGET STATE

Continuous monitoring

Current RMF control posture, vulnerabilities, assets, changes, and evidence status.

Active cyber defense context

Security findings and events can be tied back to risk actions and response workflows.

Secure software supply chain

SBOM, container findings, pipeline gates, and dependencies become part of the evidence model.

Lessons learned

Start with authoritative evidence sources • Preserve lineage • Keep AI advisory • Measure readiness, not just compliance • Expand by control family and workflow

Key takeaways

1. RMF's promise is continuous risk management, not static paperwork.
2. Security data already exists, but needs traceability to become authorization evidence.
3. AI can accelerate assurance inside IL6 when findings remain human-attested.
4. cATO readiness is built through monitored evidence, active defense context, and supply-chain visibility.

Questions

Thank you

Contact: joel.shuler@pt78.co

Built to Serve. Built to Scale.